UNIT-5
SECURITY AND ETHICAL CHALLENGES

SYLLABUS: Information Systems Controls –Risks of Online Operations –Security Measures –Systems Controls and Audits–Ethical Responsibility of Business Professionals- ERP -e-governance

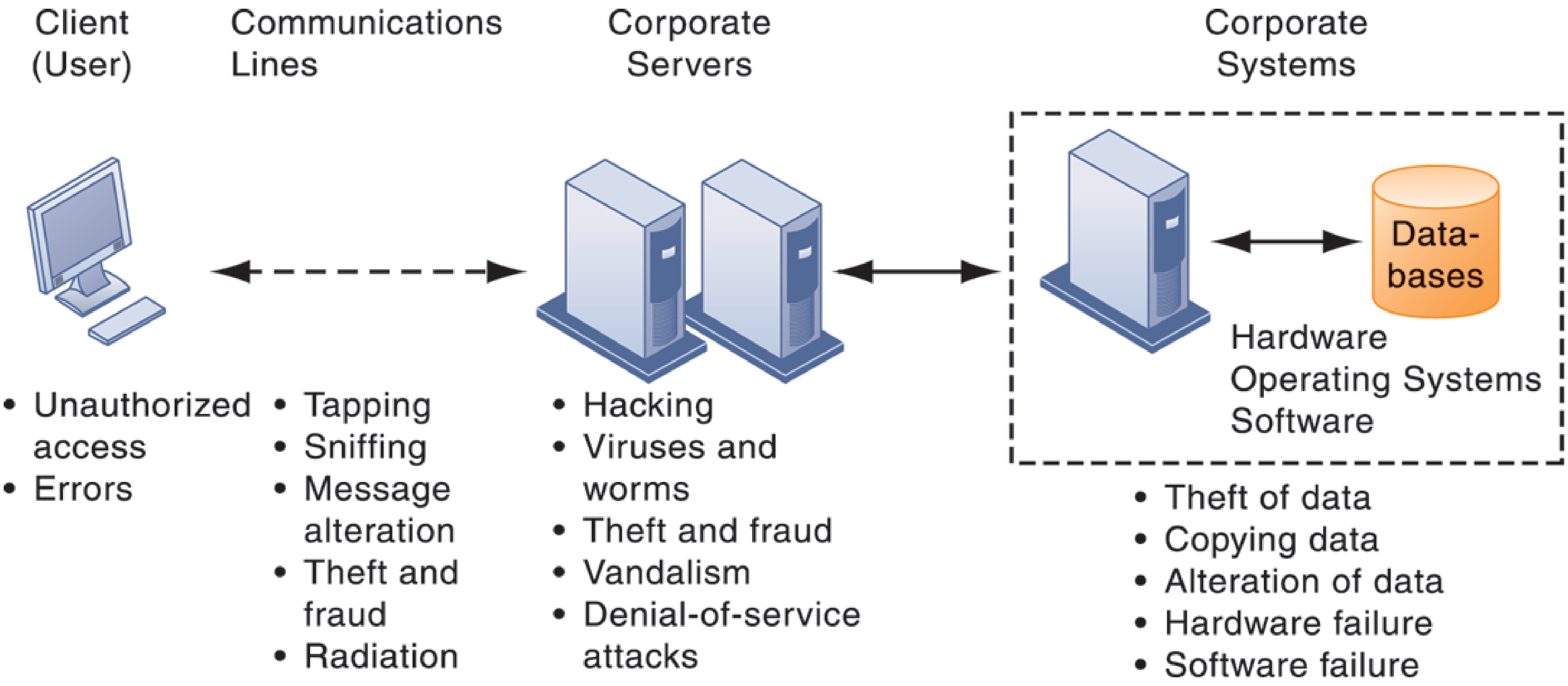
Securities Vs Control

- Security:
  - Policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems
- Controls:
  - Methods, policies, and organizational procedures that ensure safety of organization’s assets; accuracy and reliability of its accounting records; and operational adherence to management standards

Why systems are vulnerable?

- Accessibility of networks
- Hardware problems (breakdowns, configuration errors, damage from improper use or crime)
- Software problems (programming errors, installation errors, unauthorized changes)
- Disasters
- Use of networks/computers outside of firm’s control
- Loss and theft of portable devices

Types of Security Challenges & Vulnerabilities



Client (User)

- Unauthorized access
- Errors

Communications Lines

- Tapping
- Sniffing
- Message alteration
- Theft and fraud
- Radiation

Corporate Servers

- Hacking
- Viruses and worms
- Theft and fraud
- Vandalism
- Denial-of-service attacks

Corporate Systems

Hardware
Operating Systems
Software

- Theft of data
- Copying data
- Alteration of data
- Hardware failure
- Software failure

System Vulnerabilities

- Internet vulnerabilities
  - Network open to anyone
  - Size of Internet means abuses can have wide impact
  - Use of fixed Internet addresses with cable / DSL modems creates fixed targets for hackers

System Vulnerabilities - Malware (malicious software)

- Viruses
  - Rogue software program that attaches itself to other software programs or data files in order to be executed
- Worms
  - Independent programs that copy themselves from one computer to other computers over a network.
- Worms and viruses spread by
  - Downloads (drive-by downloads)
  - E-mail, attachments
  - Downloads on Web sites and social networks

System Vulnerabilities - Malware (malicious software)

- Smart phones as vulnerable as computers
  - Study finds 13,000 types of smart phone malware
- Trojan horses
  - Software that appears benign but does something other than expected. Ex : MMarketPay.A
- SQL injection attacks
  - Hackers submit data to Web forms that exploits site's unprotected software and sends rogue SQL query to database

System Vulnerabilities - Malware (malicious software)

- Spyware
  - Small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising
  - Key loggers
    - Record every keystroke on computer to steal serial numbers, passwords, launch Internet attacks
  - Other types:
    - Reset browser home page
    - Redirect search requests
    - Slow computer performance by taking up memory

System Vulnerabilities

- Hackers and computer crime
  - Hackers vs. crackers
  - Activities include:
    - System intrusion
    - System damage
    - Cybervandalism
      - destruction of Web site or corporate information system

System Vulnerabilities

- Spoofing
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
  - Redirecting Web link to address different from intended one, with site masquerading as intended destination
- Sniffer
  - Eavesdropping program that monitors information traveling over network
  - Enables hackers to steal proprietary information such as e-mail, company files, and so on

System Vulnerabilities

- Denial-of-service attacks (DoS)
  - Flooding server with thousands of false requests to crash the network
- Distributed denial-of-service attacks (DDoS)
  - Use of numerous computers to launch a DoS
  - Botnets
    - Networks of “zombie” PCs infiltrated by bot malware
    - Grum botnet: controlled 560K to 840K computers

Computer crime

- Defined as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution"
- Computer may be target of crime, for example:
  - Breaching confidentiality of protected computerized data
  - Accessing a computer system without authority
- Computer may be instrument of crime, for example:
  - Theft of trade secrets
  - Using e-mail for threats or harassment

System Vulnerabilities

- Identity theft
  - Theft of personal Information (social security ID, driver ’ s license, or credit card numbers) to impersonate someone else
- Phishing
  - Setting up fake Web sites or sending e-mail messages that look like legitimate businesses to ask users for confidential personal data.
- Evil twins
  - Wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet

System Vulnerabilities

- Pharming
  - Redirects users to a bogus Web page, even when individual types correct Web page address into his or her browser
- Click fraud
  - Occurs when individual or computer program fraudulently clicks on online ad without any intention of learning more about the advertiser or making a purchase
- Cyberterrorism and Cyberwarfare

Internal threats

- Internal threats: Employees
  - Security threats often originate inside an organization
  - Inside knowledge
  - Sloppy security procedures
    - User lack of knowledge
  - Social engineering:
    - Tricking employees into revealing their passwords by pretending to be legitimate members of the company in need of information

Internal Threats

- Software vulnerability
  - Commercial software contains flaws that create security vulnerabilities
    - Hidden bugs (program code defects)
      - Zero defects cannot be achieved because complete testing is not possible with large programs
    - Flaws can open networks to intruders
  - Patches
    - Small pieces of software to repair flaws
    - Exploits often created faster than patches can be released and implemented

Importance of Security & Control

- Failed computer systems can lead to significant or total loss of business function.
- Firms now are more vulnerable than ever.
  - Confidential personal and financial data
  - Trade secrets, new products, strategies
- A security breach may cut into a firm's market value almost immediately.
- Inadequate security and controls also bring forth issues of liability.

Importance of Security & Control

- Legal and regulatory requirements for electronic records management and privacy protection
- Electronic evidence
  - Evidence for white collar crimes often in digital form
    - Data on computers, e-mail, instant messages, e-commerce transactions
  - Proper control of data can save time and money when responding to legal discovery request
- Computer forensics:
  - Scientific collection, examination, authentication, preservation, and analysis of data from computer storage media for use as evidence in court of law
  - Includes recovery of ambient and hidden data

Information Systems Control

- Information systems controls
  - Manual and automated controls
  - General and application controls
- General controls
  - Govern design, security, and use of computer programs and security of data files in general throughout organization's information technology infrastructure
  - Apply to all computerized applications
  - Combination of hardware, software, and manual procedures to create overall control environment

Information Systems Control

- Types of general controls
  - Software controls
  - Hardware controls
  - Computer operations controls
  - Data security controls
  - Implementation controls
  - Administrative controls

Information Systems Control

- Application controls
  - Specific controls unique to each computerized application, such as payroll or order processing
  - Include both automated and manual procedures
  - Ensure that only authorized data are completely and accurately processed by that application
  - Include:
    - Input controls
    - Processing controls
    - Output controls

Establishing Information Systems Control

- Risk assessment: Determines level of risk to firm if specific activity or process is not properly controlled
    - Types of threat
    - Probability of occurrence during year
    - Potential losses, value of threat
    - Expected annual loss
- Security policy
    - Ranks information risks, identifies acceptable security goals, and identifies mechanisms for achieving these goals
    - Drives other policies
        - Acceptable use policy (AUP)
            - Defines acceptable uses of firm's information resources and computing equipment
        - Authorization policies
            - Determine differing levels of user access to information assets

Establishing Information Systems Control

- Identity management
  - Business processes and tools to identify valid users of system and control access
    - Identifies and authorizes different categories of users
    - Specifies which portion of system users can access
    - Authenticating users and protects identities
  - Identity management systems
    - Captures access rules for different levels of users

Establishing Information Systems Control

- Disaster recovery planning: Devises plans for restoration of disrupted services
- Business continuity planning: Focuses on restoring business operations after disaster
  - Both types of plans needed to identify firm's most critical systems
  - Business impact analysis to determine impact of an outage
  - Management must determine which systems restored first

MIS audit

- Examines firm’s overall security environment as well as controls governing individual information systems
- Reviews technologies, procedures, documentation, training, and personnel.
- May even simulate disaster to test response of technology, IS staff, other employees
- Lists and ranks all control weaknesses and estimates probability of their occurrence
- Assesses financial and organizational impact of each threat

Security Measures

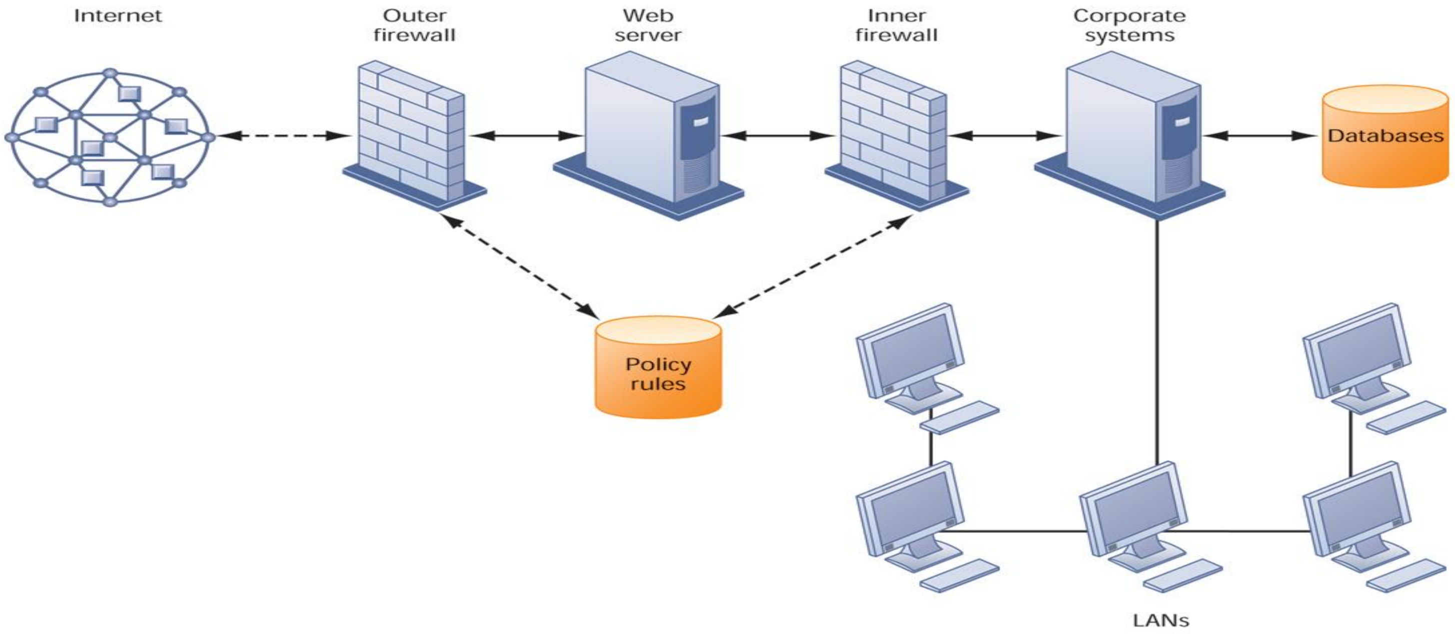
- Identity management software
  - Automates keeping track of all users and privileges
  - Authenticates users, protecting identities, controlling access
- Authentication
  - Password systems
  - Tokens
  - Smart cards
  - Biometric authentication

Security Measures

- Firewall:
  - Combination of hardware and software that prevents unauthorized users from accessing private networks
  - Technologies include:
    - Static packet filtering
    - Stateful inspection
    - Network address translation (NAT)
    - Application proxy filtering

Firewall - Example

- Here the firewall is placed between the firm’s private network and the public Internet or another distrusted network to protect against unauthorized traffic.



Security Measures

- Intrusion detection systems:
  - Monitors hot spots on corporate networks to detect and deter intruders
  - Examines events as they are happening to discover attacks in progress
- Antivirus and antispyware software:
  - Checks computers for presence of malware and can often eliminate it as well
  - Requires continual updating
- Unified threat management (UTM) systems

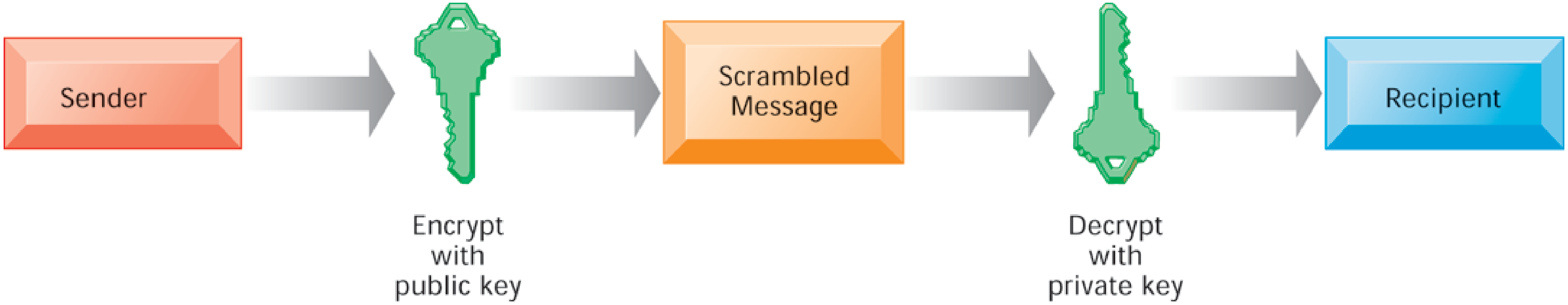
Security Measures

- Securing wireless networks
  - WEP security can provide some security by:
    - Assigning unique name to network's SSID and not broadcasting SSID
    - Using it with VPN technology
  - Wi-Fi Alliance finalized WAP2 specification, replacing WEP with stronger standards
    - Continually changing keys
    - Encrypted authentication system with central server

Security Measures

- Encryption:
  - Transforming text or data into cipher text that cannot be read by unintended recipients
  - Two methods for encryption on networks
    - Secure Sockets Layer (SSL) and successor Transport Layer Security (TLS)
    - Secure Hypertext Transfer Protocol (S-HTTP)

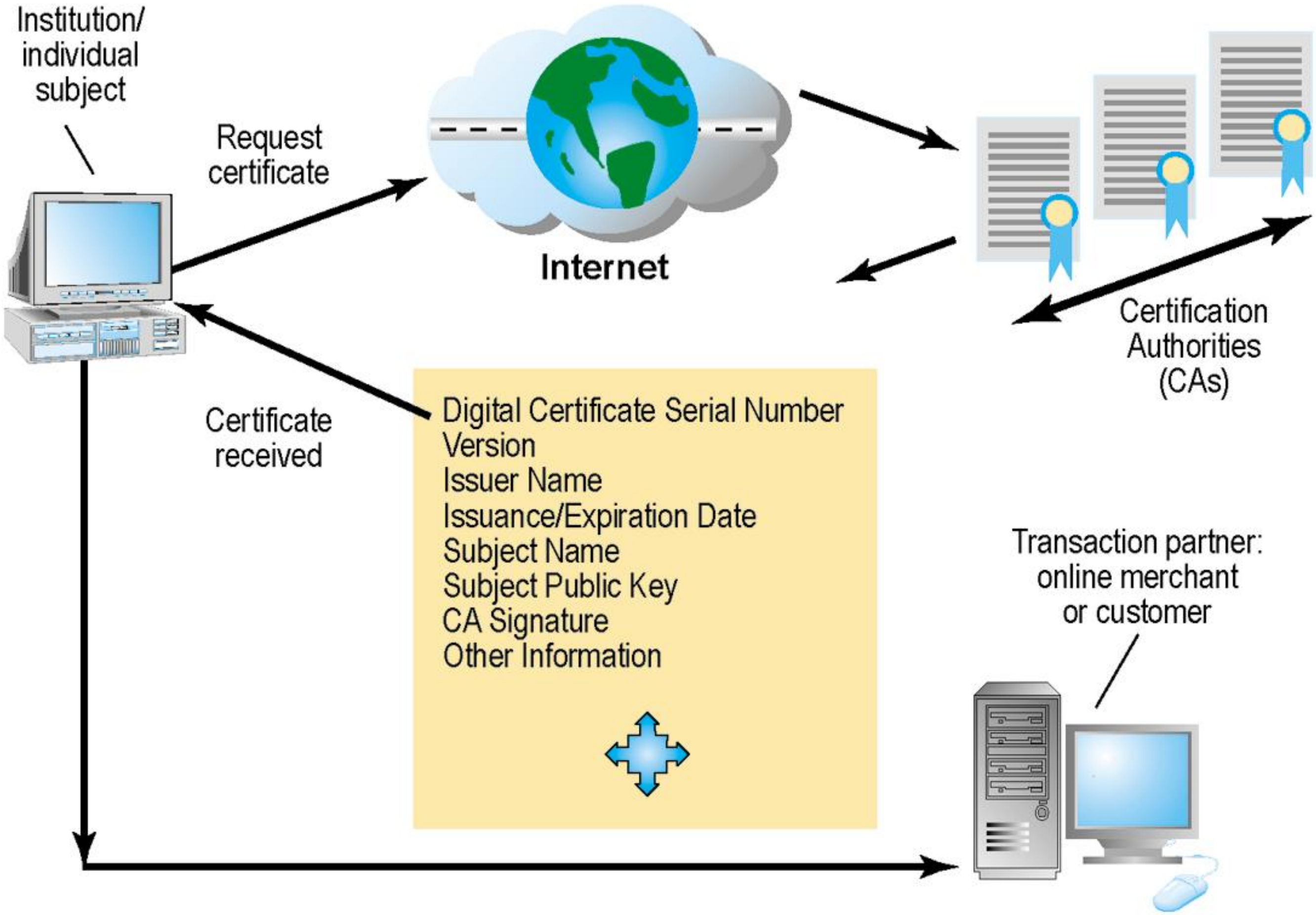
- Two methods of encryption
  - Symmetric key encryption
    - Sender and receiver use single, shared key
  - Public key encryption
    - Uses two, mathematically related keys: Public key and private key
    - Sender encrypts message with recipient’s public key



Security Measures

- Digital certificate:
  - Data file used to establish the identity of users and electronic assets for protection of online transactions
  - Uses a trusted third party, certification authority (CA), to validate a user's identity
  - CA verifies user's identity, stores information in CA server, which generates encrypted digital certificate containing owner ID information and copy of owner's public key
- Public key infrastructure (PKI)
  - Use of public key cryptography working with certificate authority
  - Widely used in e-commerce

Digital Certificates



Digital Certificate Serial Number
Version
Issuer Name
Issuance/Expiration Date
Subject Name
Subject Public Key
CA Signature
Other Information

Security Measures

- Ensuring system availability
  - Online transaction processing requires 100% availability, no downtime
- Fault-tolerant computer systems
  - For continuous availability, for example, stock markets
  - Contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service
- High-availability computing
  - Helps recover quickly from crash
  - Minimizes, does not eliminate, downtime

Security Measures

- Recovery-oriented computing
  - Designing systems that recover quickly with capabilities to help operators pinpoint and correct faults in multi-component systems
- Controlling network traffic
  - Deep packet inspection (DPI)
    - Video and music blocking
- Security outsourcing
  - Managed security service providers (MSSPs)

Security Measures

- Security in the cloud
  - Responsibility for security resides with company owning the data
  - Firms must ensure providers provides adequate protection:
    - Where data are stored
    - Meeting corporate requirements, legal privacy laws
    - Segregation of data from other clients
    - Audits and security certifications
  - Service level agreements (SLAs)

Security Measures

- Securing mobile platforms
  - Security policies should include and cover any special requirements for mobile devices
    - Guidelines for use of platforms and applications
  - Mobile device management tools
    - Authorization
    - Inventory records
    - Control updates
    - Lock down/erase lost devices
    - Encryption
  - Software for segregating corporate data on devices

Security Measures

- Ensuring software quality
  - Software metrics: Objective assessments of system in form of quantified measurements
    - Number of transactions
    - Online response time
    - Payroll checks printed per hour
    - Known bugs per hundred lines of code
  - Early and regular testing
  - Walkthrough: Review of specification or design document by small group of qualified people
  - Debugging: Process by which errors are eliminated

Ethical Responsibilities of Business Professionals

- Ethics refers to rules of right and wrong that people use to make choices to guide their behaviours.
- Ethics in MIS seek to protect and safeguard individuals and society by using information systems responsibly.
- Most professions usually have defined a code of ethics or code of conduct guidelines that all professionals affiliated with the profession must adhere to.
- Following organizations promote ethical issues −
  - The Association of Information Technology Professionals (AITP)
  - The Association of Computing Machinery (ACM)
  - The Institute of Electrical and Electronics Engineers (IEEE)
  - Computer Professionals for Social Responsibility (CPSR)

Information Communication Technology (ICT) Process

- An ICT policy is a set of guidelines that defines how an organization should use information technology and information systems responsibly.
- ICT policies usually include guidelines on:
  - Purchase and usage of hardware equipment and how to safely dispose them
  - Use of licensed software only and ensuring that all software is up to date with latest patches for security reasons
  - Rules on how to create passwords (complexity enforcement), changing passwords, etc.
  - Acceptable use of information technology and information systems
  - Training of all users involved in using ICT and MIS

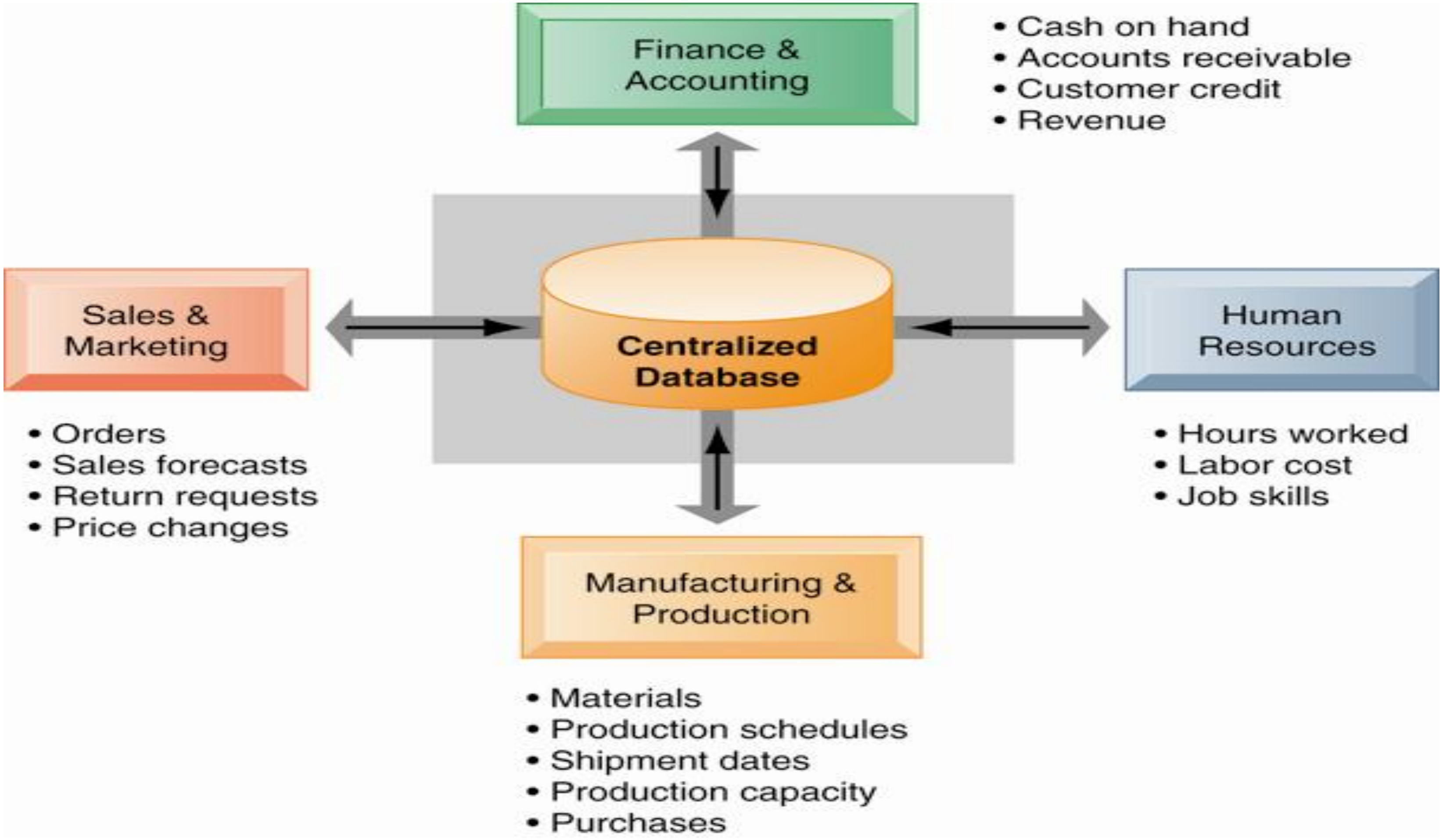
ERP

- Enterprise resource planning (ERP) systems
- Suite of integrated software modules and a common central database
- Collects data from many divisions of firm for use in nearly all of firm’s internal business activities
- Information entered in one process is immediately available for other processes

ERP

- Enterprise Software
  - Built around thousands of predefined business processes that reflect best practices
    - Finance and accounting
    - Human resources
    - Manufacturing and production
    - Sales and marketing
  - To implement, firms:
    - Select functions of system they wish to use.
    - Map business processes to software processes.
      - Use software’s configuration tables for customizing.

How Enterprise System works?



ERP

- Business value of enterprise systems
  - Increase operational efficiency
  - Provide firm-wide information to support decision making
  - Enable rapid responses to customer requests for information or products
  - Include analytical tools to evaluate overall organizational performance

ERP: Challenges & Opportunities

- Enterprise application challenges
  - Highly expensive to purchase and implement enterprise applications
    - Average “large” system—$12 million +
    - Average “small/midsize” system—$3.5 million
  - Technology changes
  - Business process changes
  - Organizational learning, changes
  - Switching costs, dependence on software vendors
  - Data standardization, management, cleansing

ERP: Challenges & Opportunities

- Next-generation enterprise applications
  - Enterprise solutions/suites:
    - Make applications more flexible, Web-enabled, integrated with other systems
  - SOA standards
  - Open-source applications
  - On-demand solutions
  - Cloud-based versions
  - Functionality for mobile platform

ERP: Challenges & Opportunities

- Social CRM
  - Incorporating social networking technologies
  - Company social networks
  - Customer interaction via Facebook
- Business intelligence
  - Inclusion of BI with enterprise applications
  - Flexible reporting, ad hoc analysis, "what-if" scenarios, digital dashboards, data visualization

E-governance

- **Definition**: E-governance, expands to **electronic governance**, is the integration of **Information and Communication Technology (ICT)** in all the processes, with the aim of enhancing government ability to address the needs of the general public.
- The basic purpose of e-governance is to simplify processes for all, i.e. government, citizens, businesses, etc. at National, State and local levels.

E-governance

- In short, it is the use of electronic means, to **promote good governance**.
- It connotes the implementation of information technology in the government processes and functions so as to cause **simple, moral, accountable and transparent governan**ce.
- It entails the access and delivery of government services, dissemination of information, communication in a quick and efficient manner.

Benefits of E-governance

- Reduced corruption
- High transparency
- Increased convenience
- Growth in GDP
- Direct participation of constituents
- Reduction in overall cost.
- Expanded reach of government

Types of Interactions in E-Governance

- G2G (Government to Government)
- G2C (Government to Citizen)
- G2B (Government to Business)
- G2E (Government to Employees)

E-governance : opportunities & challenges

- E-governance can only be possible if the government is ready for it.
- It is not a one day task, and so the government has to make plans and implement them before switching to it.
- Some of the measures include Investment in telecommunication infrastructure, budget resources, ensure security, monitor assessment, internet connectivity speed, promote awareness among public regarding the importance, support from all government departments and so forth.
- E-governance has a great role to play, that **improves and supports all tasks performed by the government department and agencies,** because it simplifies the task on the one hand and increases the quality of work on the other.